PRÁCE S DATY KONCOVÝCH UŽIVATELŮ LIVESUPP

Veškerá komunikace se službou LiveSupp probíhá výhradně přes HTTPS, tedy přes šifrované spojení pomocí TLS ECDHE RSA with AES 128 GCM SHA256. Takto je šifrovaná i následná P2P komunikace mezi Operátory a koncovými uživateli případně Operátory a Operátory (v rámci interní komunikace).

PŘÍSTUP K DATŮM

Databáze běží na našich dedikovaných serverech, nevyužíváme cloudových služeb externích dodavatelů a ani do budoucna neplánujeme. Z toho vyplývá, že k databázi může mít přístup buď server admin nebo admin vývojář. Další informace je možné sdělit na vyžádání.

DATA KONCOVÝCH UŽIVATELŮ

Data koncových uživatelů jsou uloženy v šifrované podobě pomocí DEK (data-encryption-key) – generace klíče se děje pomocí CSPRNG. Uživatelům se po zadání hesla vygeneruje KEK (key-encryption-key), za pomoci několika iterací hashovací funkce Bcrypt a „soli“. KEK se potom využije k zašifrování DEK a ten se zašifrovaný uloží do databáze. Při přihlášení se potom uživatelské heslo a sůl použije pro vygenerování KEK, který rozšifruje DEK, pomocí nějž je možné rozšifrovat data.

Takto se šifruje veškerá textová komunikace mezi operátory a koncovými uživateli a operátory s operátory (interní komunikace), uložená data operátory ke koncovým uživatelům (například jméno, e-mail, telefon, poznámka), další informace o koncových uživatelích, jako je IP adresa, poloha atd.

Data, která neukládáme a nemáme možnost ukládat, jelikož běží přes P2P kanál, jsou následující:

Obsah real-time hovorů (video, hlas) + nahrávky těchto spojení, Screensharingové spojení, poslané soubory.

Pro cobrowsingové spojení koncového uživatele a operátora je použita komunikace ve stylu koncový uživatel-server-operátor. Spojení je šifrováno pomocí SSL, stejně jako veškerá ostatní komunikace. Z těchto spojení momentálně neukládáme žádná data, krom záznamu o tom, že ke spojení došlo.

Po ukončení Screenshare (sdílení obrazovky), Cobrowsing (sdílení stránek) nebo hlasového a video spojení nemůže operátor znovu zahájit toto spojení bez potvrzení koncového uživatele.

VALIDACE VSTUPŮ

Probíhá primárně na stranách koncového uživatele a operátora (v případech datového toku koncový uživatel-operátor). Pokud se jedná o komunikaci koncový uživatel-server-operátor, tak jsou data validována ještě na serveru.

Použité mechanismy validace vstupů

- kontrolujeme strukturu dat, která k nám na server proudí od uživatelů
- escapujeme data při komunikací s databází, čímž bráníme sql injection
- escapujeme data při vykreslování v browseru, čímž bráníme xss injection
- při cobrowsingu spouštíme stránku u operátora v sandboxu ve dvou iframech a navíc na serveru odfiltrováváme jakýkoliv javascript, který by se mu klient snažil podsunout